Using SELinux to Enforce Two-Dimensional Labelled Security Model with Partially Trusted Subjects

Autor: ***Martin Jurčík***
Vedúci práce: ***RNDr. Jaroslav Janáček, PhD.***

Fakulta matematiky, fyziky a informatiky
Univerzita Komenského
Bratislava

Cieľ našej práce:

Naším cieľom bolo implementovať bezpečnostný model pomocou SELinux mechanizmu. Chceli sme zlepšiť implementáciu prezentovanú v bakalárskej práci a to pomocou Multi-Level Security prostriedkov. Následne sme chceli rozšíriť samotný SELinux o náš model.

Bezpečnostný model

Bezpečnostný model navrhol RNDr. Jaroslav Janáček, PhD. v jeho dizertačnej práci. Tento model je kombináciou Bell-La Padula a Biba modelov. Model rozdeľuje entity OS na objekty a subjekty, pričom subjekty sú ďalej rozdelené na dôveryhodné, nedôveryhodné a čiastočne dôveryhodné. Každej entite model priraďuje úroveň dôvernosti, integrity a štítok (label).

SELinux

Security-Enhanced Linux (SELinux) je bezpečnostný modul, ktorý tvorí nadstavbu štandardného bezpečnostného modelu v OS Linux. Obsahuje vlastné definície používateľov. Bezpečnostný kontext tvoria identita používateľa, jeho úloha v systéme, typ danej entity a bezpečnostná úroveň, ktorú sme použili na implementáciu nášo modelu. Táto bezpečnostná úroveň využíva prostriedky Multi Level Security (MLS), prípadne jej špeciálnu formu, ktorou je Multi-Category Security (MCS).

Naše riešenie

Finálne riešenie nesie názov MCS-4.0. Všetky atribúty kódujeme do kategórií. Takýmto riešením sme dosiahli zlúčenie dvoch rôznych politík. Nielenže vieme rozšíriť ľubovoľnú existujúcu bezpečnostnú politiku pre SELinux využívajúcu aj MLS (prípadne iba MCS) o náš model, ale získali sme aj efektívnejšiu implementáciu a v neposlednom rade aj ľahšie nasadenie. Na rozdiel od implementácie prezentovanej v našej bakalárskej práci sa nám podarilo dosiahnúť konštantnú dĺžku pravidiel pre realizáciu nášho bezpečnostného modelu, bezpečnostný kontext je priradený priamo entite a nie iba typu entity a implementovali sme aj automatický kontext novovytváraného objektu. Aktuálna implementácia podporuje až 8 úrovní pre dôvernosť a integritu a až 64 štítkov (labels).